A. Use the definition for a ring to prove that Z_5 is a ring under the operations + and × defined as follows:

$$[a]_5 + [b]_5 = [a + b]_5 \text{ and } [a]_5 \times [b]_5 = [a \times b]_5$$

Start with the a set and two operations:

$$Z_5 = < \{0, 1, 2, 3, 4\}, +_5, \times_5 >$$

Define each element according to their congruence classes:

$0 = [0]_5$, $1 = [1]_5$, $2 = [2]_5$, $3 = [3]_5$, and $4 = [4]_5$

The Cayley table for multiplication modulus-5:

Table 1. ALL POSSIBLE PRODUCTS

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The Cayley table for addition modulus-5:

Table 2. ALL POSSIBLE SUMS

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

To prove Z_5 is a ring, we show *closure*, *identity*, *additive inverses*, *commutative under addition*, and *associative* for each operation. We also must prove the *distributive* property is satisfied.

Closure Under Multiplication

We show that for every $a, b \in Z_5$, the product $a \times b \in Z_5$. The elements of the set are $\{0, 1, 2, 3, 4\}$ and all the possible products are in the Cayley table. There are no products outside the set. That is, whenever we multiply any of the set elements of Z_5 we get an answer that is also in the same set. Therefore, Z_5 is closed under multiplication.

Closure Under Addition

NOT SHOWN: Finish using closure under multiplication as an example

Multiplicative Identity

NOT SHOWN: Finish using additive identity as an example

Additive Identity

There is an element $[0]_5 \in Z_5$ such that for every $[a]_5 \in Z_5$,

$$[0]_5 + [a]_5 = [a]_5 + [0]_5 = [a]_5$$

$[0]_5 + [0]_5 = [0]_5$	• $a = 0$
$[0]_5 + [1]_5 = [1]_5 + [0]_5 = [1]_5$	• $a = 1$
$[0]_5 + [2]_5 = [2]_5 + [0]_5 = [2]_5$	• $a = 2$
$[0]_5 + [3]_5 = [3]_5 + [0]_5 = [3]_5$	• $a = 3$
$[0]_5 + [4]_5 = [4]_5 + [0]_5 = [4]_5$	• $a = 4$

Since $[0]_5 + [a]_5 = [a]_5 + [0]_5 = [a]_5$ for every $a \in Z_5$, we found the additive identity to be the element $a = 0$ which is contained in the set Z_5.

Additive Inverses

For each element $[a]_5 \in Z_5$, there is an element $[b]_5 \in Z_5$ such that $[a]_5 + [b]_5 = [0]_5$. That is, for each element in the set, there is another element also in the set, such that their sum is equal to the additive identity.

$[0]_5 + [0]_5 = [0]_5$	• means that 0 is the additive inverse of 0
$[1]_5 + [4]_5 = [0]_5$	• means that 4 is the additive inverse of 1
$[2]_5 + [3]_5 = [0]_5$	• means that 3 is the additive inverse of 2
$[3]_5 + [2]_5 = [0]_5$	• means that 2 is the additive inverse of 3
$[4]_5 + [1]_5 = [0]_5$	• means that 1 is the additive inverse of 4

Since all the additive inverses are also members of the set $\{0, 1, 2, 3, 4\}$, we know that Z_5 is closed with respect to additive inverses. That is, for every element in the set Z_5, there is an additive inverse element that is also in the set.

Associative under Addition

NOT SHOWN: Finish using associative under multiplication as an example

Associative under Multiplication

Let a, b, c be arbitrary elements of Z_5 be represented by their corresponding congruence classes modulus-5 as $[a]_5, [b]_5,$ and $[c]_5$ respectively. To show that the elements are associative under multiplication, we show:

$$([a]_5 \times [b]_5) \times [c]_5 \; = \; [a]_5 \times ([b]_5 \times [c]_5)$$

$$([a]_5 \times [b]_5) \times [c]_5 = ([a \times b]_5) \times [c]_5$$
- definition of modular multiplication

$$= [(a \times b) \times c]_5$$
- definition of modular multiplication

$$= [a \times (b \times c)]_5$$
- integers associative under multiplication

$$= [a]_5 \times ([b \times c]_5)$$
- definition of modular multiplication

$$= [a]_5 \times ([b]_5 \times [c]_5)$$
- integers associative under multiplication

Commutative under Addition

Let a, b be arbitrary elements of Z_5 be represented by their corresponding congruence classes modulus-5 as $[a]_5$, and $[b]_5$ respectively. To show that the elements are commutative under addition, we show:

$$[a]_5 + [b]_5 = [b]_5 + [a]_5$$

$$[a]_5 + [b]_5 = [a + b]$$
- definition of modular addition

$$= [b + a]$$
- integers are commutative

$$= [b]_5 + [a]_5$$
- definition of modular addition

Left Distributive

Let a, b, c be arbitrary elements of Z_5 be represented by their corresponding congruence classes modulus-5 as $[a]_5, [b]_5$, and $[c]_5$ respectively. To show that the elements are left distributive, we show:

$$[a]_5 \times ([b]_5 + [c]_5) = ([a]_5 \times [b]_5) + ([a]_5 \times [c]_5)$$

$$[a]_5 \times ([b]_5 + [c]_5) = [a]_5 \times [b + c]_5$$
- definition of modular addition

$$= [a \times (b + c)]_5$$
- definition of modular multiplication

$$= [(a \times b) + (a \times c)]_5$$
- distributive property of integers

$$= [a \times b]_5 + [a \times c]_5$$
- definition of modular addition

$$= ([a]_5 \times [b]_5) + ([a]_5 \times [c]_5)$$
- definition of modular multiplication

Right Distributive

Let a, b, c be arbitrary elements of Z_5 be represented by their corresponding congruence classes modulus-5 as $[a]_5, [b]_5$, and $[c]_5$ respectively. To show that the elements are right distributive, we show:

$$([a]_5 \times [b]_5) + ([a]_5 \times [c]_5) = [a]_5 \times ([b]_5 + [c]_5)$$

NOT SHOWN: Finish right distributive using left distributive as an example

$\longrightarrow$ This establishes the set of integers modulus-5 under addition and multiplication is a ring.

Disclaimer

This document is meant to provide an example to aide in understanding of concepts. Read only to gain greater understanding of the concepts. Review the definition of each concept in the textbook and adopt related properties. In other words, once understood, set this example aside, do not quote, and complete a similar task in your own words.